Mobile Spam
Status and Issues

Alex Bobotek
AT&T Labs
March 15, 2016

Overview

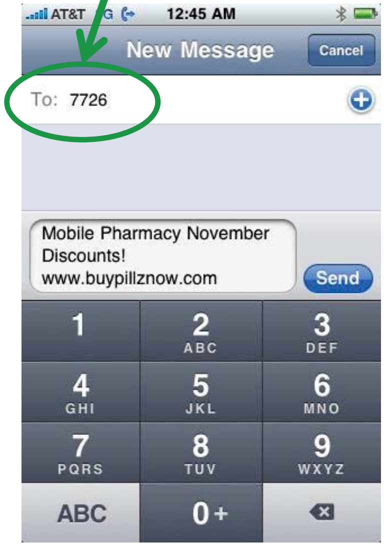
- Evolution of North American wireless SMS spam
- 2013: Initial wireless spam mitigation
- 2014: The growth of Over-the Top (OTT) SMS spam
- How spam is controlled, blocking and rate limiting A2P
- False positive incidents
- Industry guideline development
- Technical impact of regulation

New for 2010: 7726 Spam Reporting

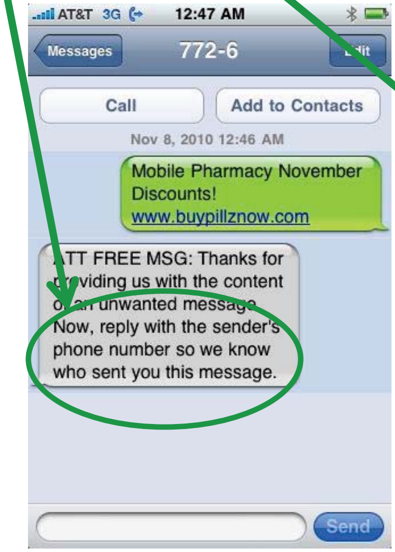
Subscriber's abuse report (example)

1. Subscriber forwards spam to 7726 ('SPAM')
2. 7726 system asks subscriber 'who sent it?'
3. Subscriber supplies abuser's MSISDN

Spam management process: deactivate/block



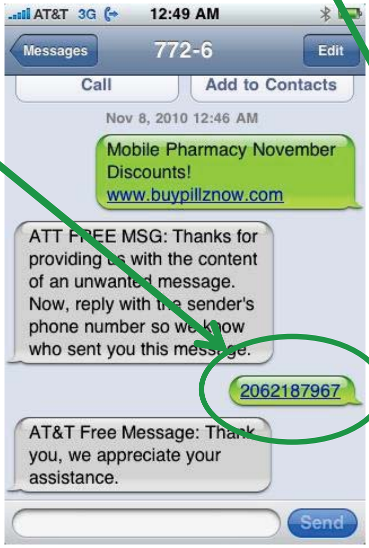
Mobile Pharmacy November Discounts! www.buypillznow.com



Nov 8, 2010 12:46 AM

Mobile Pharmacy November Discounts! www.buypillznow.com

ATT FREE MSG: Thanks for providing us with the content of an unwanted message. Now, reply with the sender's phone number so we know who sent you this message.



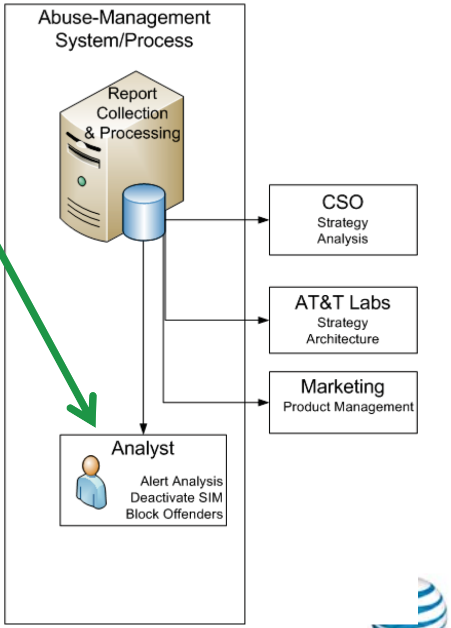
Nov 8, 2010 12:46 AM

Mobile Pharmacy November Discounts! www.buypillznow.com

ATT FREE MSG: Thanks for providing us with the content of an unwanted message. Now, reply with the sender's phone number so we know who sent you this message.

2062187967

AT&T Free Message: Thank you, we appreciate your assistance.



Abuse-Management System/Process

Report Collection & Processing

CSO
Strategy
Analysis

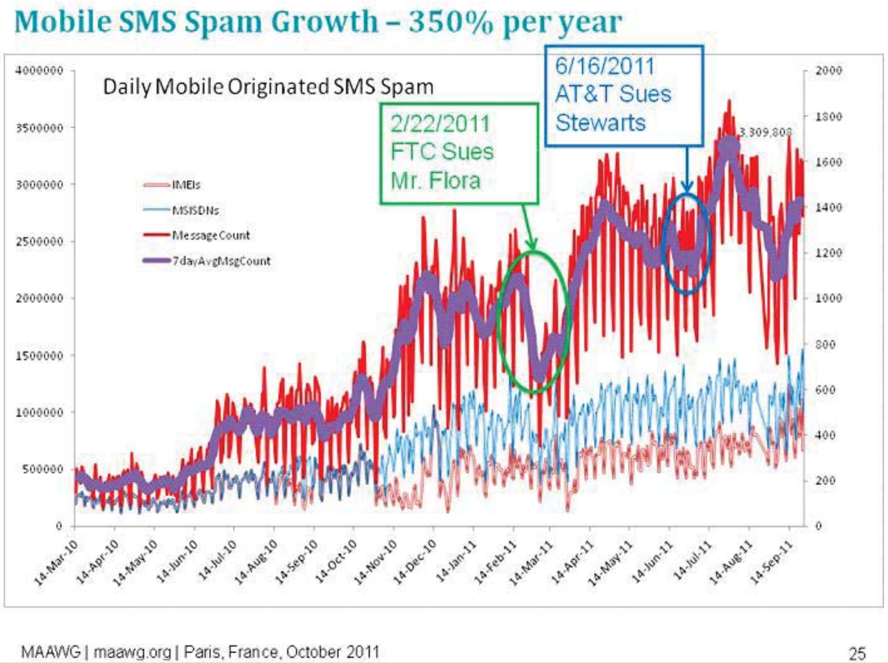
AT&T Labs
Strategy
Architecture

Marketing
Product Management

Analyst
Alert Analysis
Deactivate SIM
Block Offenders

North American SMS Spam Before 2012

- **Mobile spam and malware grew because our then-current defenses could not break the attackers' business cases**



Mobile SMS Spam Growth – 350% per year

MAAWG | maawg.org | Paris, France, October 2011

25

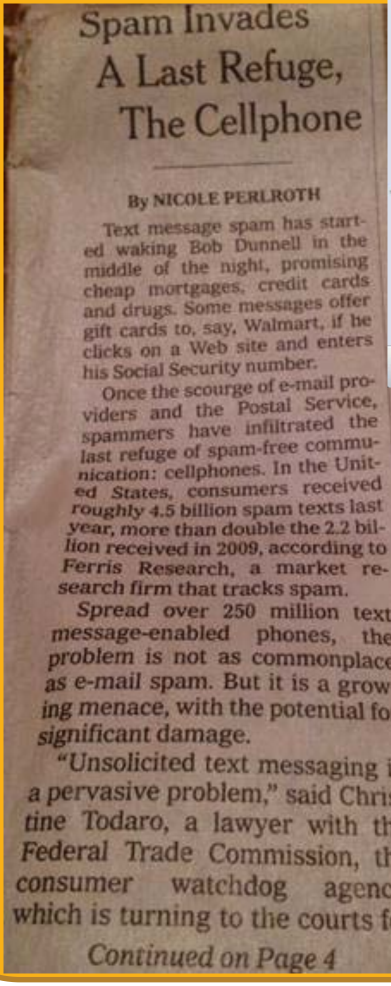
- **SIM Shutdown**

- Detect by 7726 spam reporting
- Shut down SIMs after 5-10 days
- Attacker buys new SIMs
- Spam continues

- **Lawsuits**
  - Spammer sued after ~ 1 year
  - Spammer stops for 1 week
  - Spam continues

2012: "Apple is looking for people to test & keep iPhone 5"

New York Times Front Page 4/8/12



Spam Invades A Last Refuge, The Cellphone

By NICOLE PERLROTH

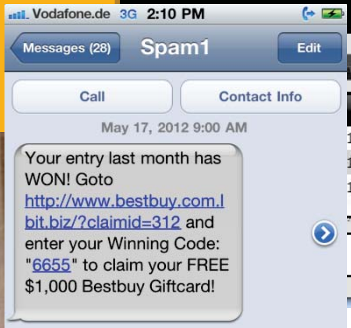
Text message spam has started waking Bob Dunnell in the middle of the night, promising cheap mortgages, credit cards and drugs. Some messages offer gift cards to, say, Walmart, if he clicks on a Web site and enters his Social Security number.

Once the scourge of e-mail providers and the Postal Service, spammers have infiltrated the last refuge of spam-free communication: cellphones. In the United States, consumers received roughly 4.5 billion spam texts last year, more than double the 2.2 billion received in 2009, according to Ferris Research, a market research firm that tracks spam.

Spread over 250 million text message-enabled phones, the problem is not as commonplace as e-mail spam. But it is a growing menace, with the potential for significant damage.

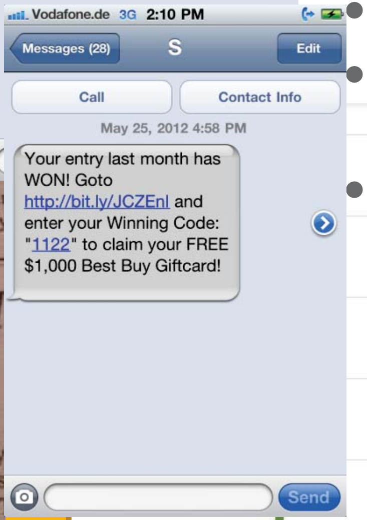
"Unsolicited text messaging is a pervasive problem," said Christine Todaro, a lawyer with the Federal Trade Commission, the consumer watchdog agency, which is turning to the courts for

Continued on Page 4



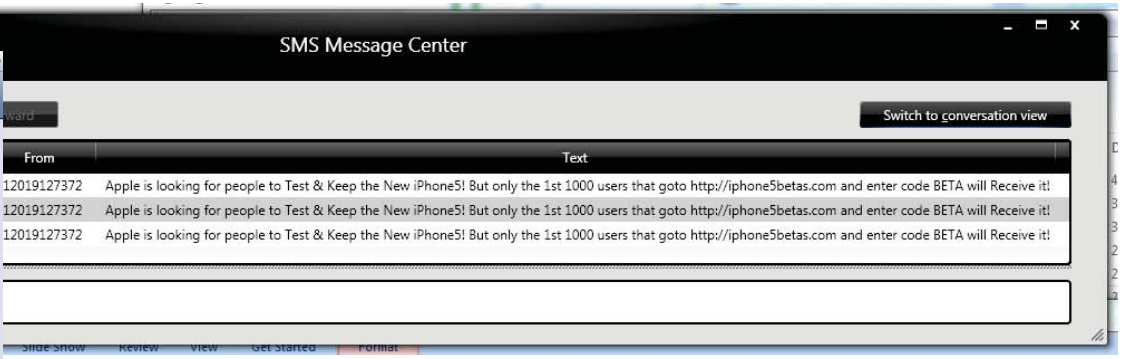
May 17, 2012 9:00 AM

Your entry last month has WON! Goto http://www.bestbuy.com.lbit.biz/?claimid=312 and enter your Winning Code: "6655" to claim your FREE $1,000 Bestbuy Giftcard!



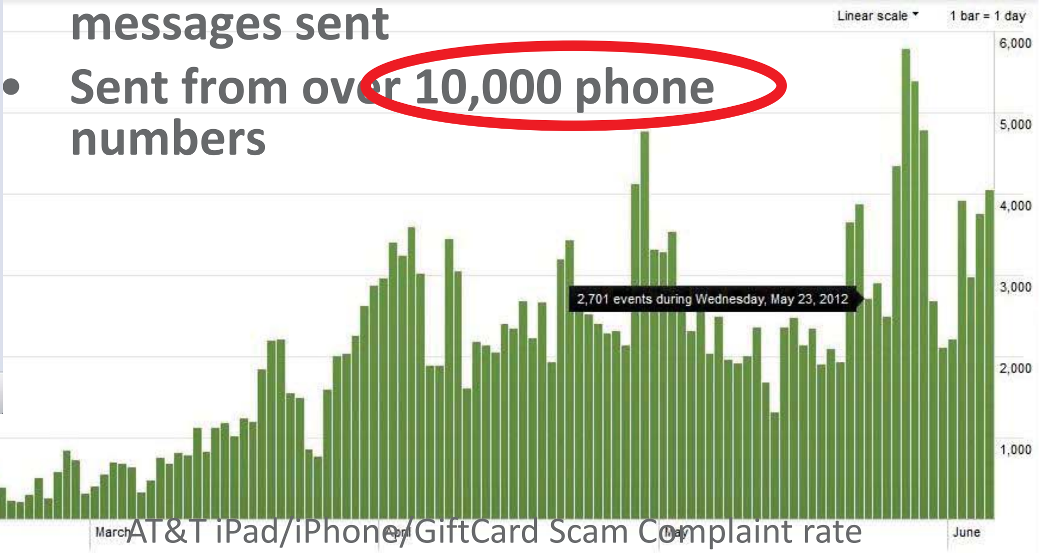
May 25, 2012 4:58 PM

Your entry last month has WON! Goto http://bit.ly/JCZEnl and enter your Winning Code: "1122" to claim your FREE $1,000 Best Buy Giftcard!



From	Text
12019127372	Apple is looking for people to Test & Keep the New iPhone5! But only the 1st 1000 users that goto http://iphone5betas.com and enter code BETA will Receive it!
12019127372	Apple is looking for people to Test & Keep the New iPhone5! But only the 1st 1000 users that goto http://iphone5betas.com and enter code BETA will Receive it!
12019127372	Apple is looking for people to Test & Keep the New iPhone5! But only the 1st 1000 users that goto http://iphone5betas.com and enter code BETA will Receive it!

- 300+ new SIMs/day
- Over 200,000,000 similar messages sent
- Sent from over 10,000 phone numbers



AT&T iPad/iPhone/GiftCard Scam Complaint rate

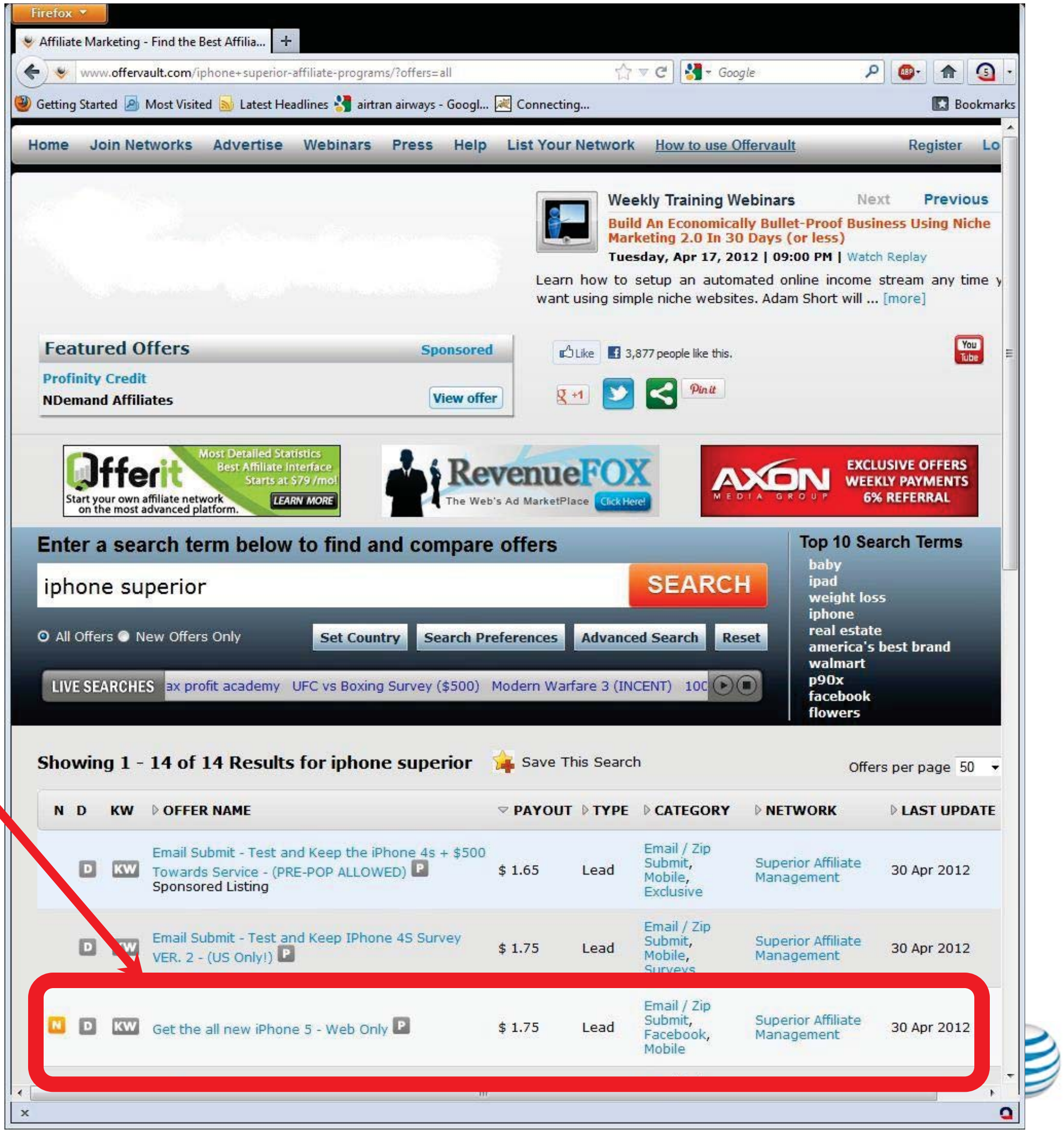
1 complaint per ~2400 spam messages

Affiliate Spam – Why SMS Spam Exploded in 2012

How to make $$$ off spam and blame someone else

- Create a fly-by-night “Incredible Offer” web site
- “Free $1000 gift card” or similar if you just sign up for this program and give us your credit card #
- “Affiliate” spammers advertise website and get $1.75 for each subscriber that visits your “Incredible Offer”

- Defenses failed
  - Internet anonymity
  - Unlimited messaging from $15 prepaid SIM



Weekly Training Webinars

Build An Economically Bullet-Proof Business Using Niche Marketing 2.0 In 30 Days (or less)

Tuesday, Apr 17, 2012 | 09:00 PM | Watch Replay

Learn how to setup an automated online income stream any time y want using simple niche websites. Adam Short will ... [more]

3,877 people like this.

Featured Offers — Sponsored

Profinity Credit

NDemand Affiliates — View offer

Enter a search term below to find and compare offers

iphone superior

● All Offers ○ New Offers Only

ax profit academy   UFC vs Boxing Survey ($500)   Modern Warfare 3 (INCENT)   10C

Top 10 Search Terms
baby
ipad
weight loss
iphone
real estate
america's best brand
walmart
p90x
facebook
flowers

Showing 1 - 14 of 14 Results for iphone superior

N	D	KW	OFFER NAME	PAYOUT	TYPE	CATEGORY	NETWORK	LAST UPDATE
	D	KW	Email Submit - Test and Keep the iPhone 4s + $500 Towards Service - (PRE-POP ALLOWED) P Sponsored Listing	$ 1.65	Lead	Email / Zip Submit, Mobile, Exclusive	Superior Affiliate Management	30 Apr 2012
	D	KW	Email Submit - Test and Keep IPhone 4S Survey VER. 2 - (US Only!) P	$ 1.75	Lead	Email / Zip Submit, Mobile, Surveys	Superior Affiliate Management	30 Apr 2012
N	D	KW	Get the all new iPhone 5 - Web Only P	$ 1.75	Lead	Email / Zip Submit, Facebook, Mobile	Superior Affiliate Management	30 Apr 2012

US Domestic Spam Status

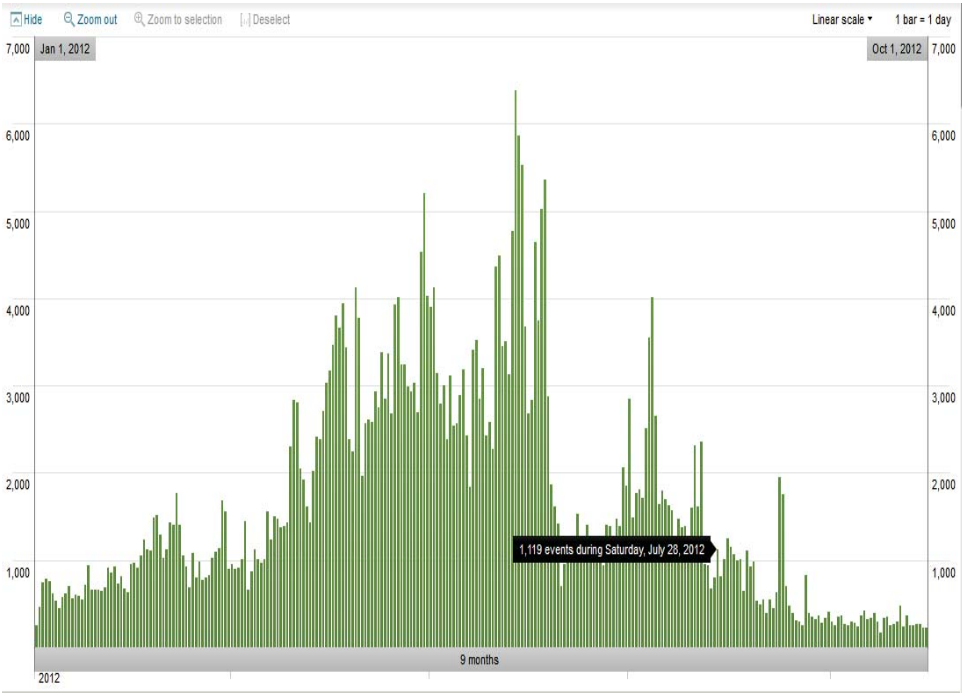
Brought Under Control in 2012 Q4

- Spam termination below pre-storm levels
- **Improved defense is responsible**
  - ○ Automatic detection & shutdown
  - ○ Improved 7726 reporting
  - ○ Bulk SIM availability/cost
  - ○ Reseller control
  - ○ Manual backup (Fraud)

- **7726 Reporting ratio improvement**
  - **1 complaint per 602 spam messages (9/20)**
  - **5 times the September 2011 rate**

- **Cautions:**
  - **Spammers may return with new methods**
  - **Current defense methods are ineffective against infected phones and compromised CPM web accounts**
    - **China has active mobile botnet of > 100k phones**
    - **GGtracker malware infected > 250k US phones**

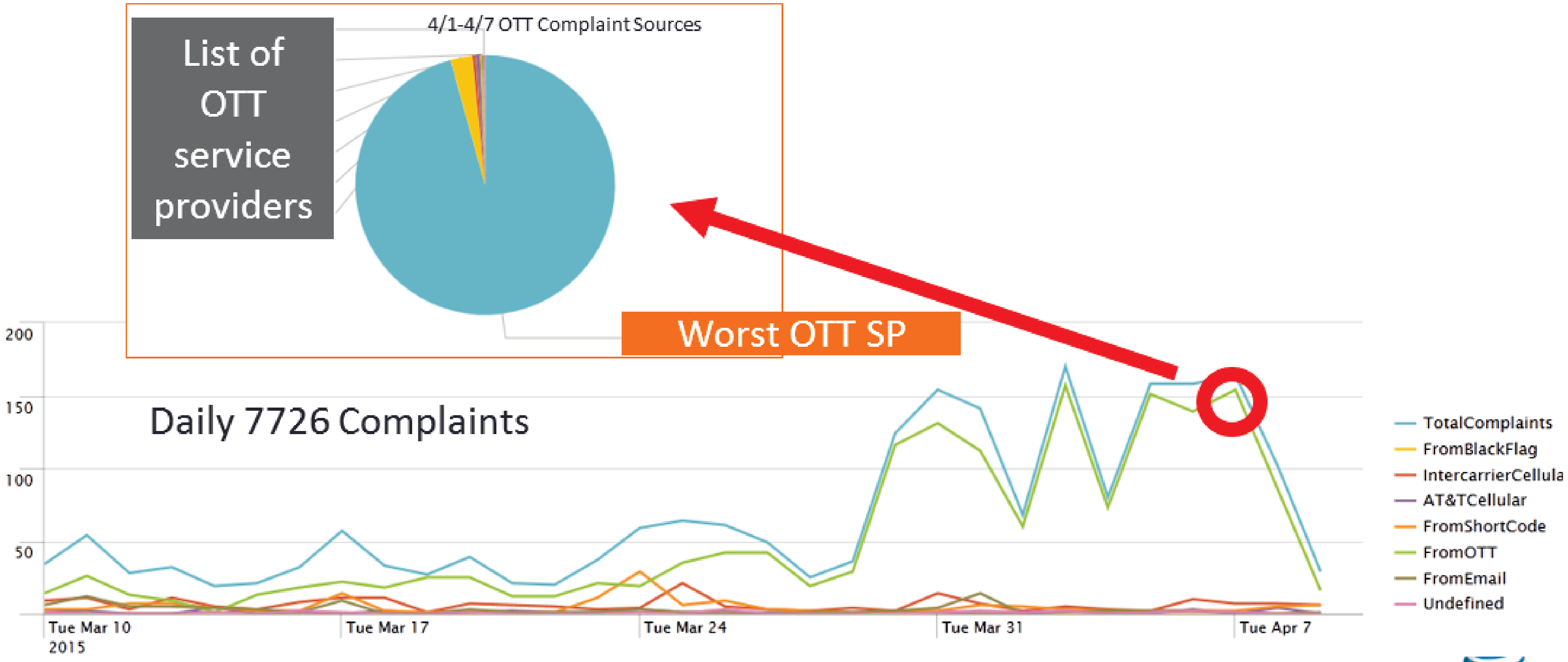
2012 AT&T 7726 Complaints (daily)



The Rise of Over-the-Top Spam

- Top spammer: OTT Service Provider
  - 1% of traffic
  - 84% of complaints (on 4/8)
  - 4/8/2015: Discussions with high-level OTT SP staff
  - 4/9/2015: Much improved, but not pristine

- Boeing Employees Credit Union security ALERT! Member: 2062[redacted]1. Urgent CALL : (866) 625-1920
- Best Deal! Take Your 5OFF On Pills! Use 5-off http://goo.gl/kX0h7P
- PromoCode-5-off. Lucky Discount on all Meds Here http://goo.gl/EAQH8D
- Special 5OFF Deal On All Meds! Code 5-off http://goo.gl/CcUvRJ
- JackpotGrand gives away 40$ No Deposit bonus tap: http://goo.gl/C1AFdT Redeem Code: RTR40
- Surprise 40$ on the house Code: RTR40 use it now: http://goo.gl/ML4xPM



List of OTT service providers

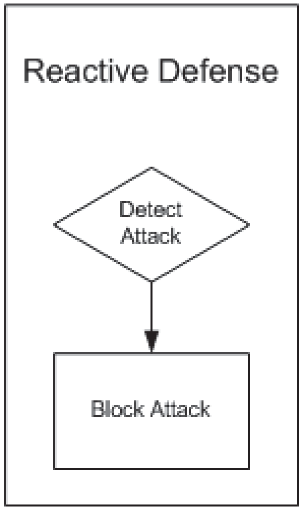
Worst OTT SP

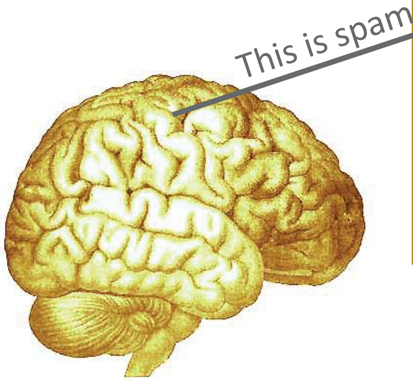
Daily 7726 Complaints

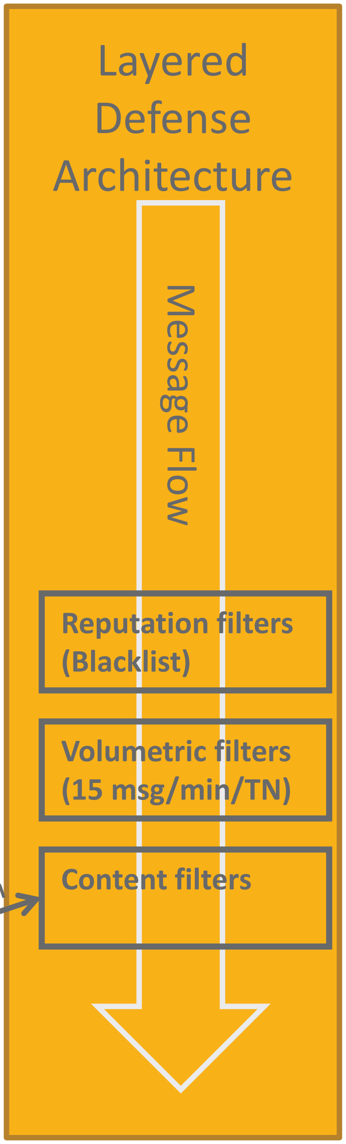
Controlling OTT Spam:
Intercarrier Long Code Spam Defenses

Three Layer Defense

- Block all messages from blacklisted numbers
  - Blacklist built based on content and volumetric history
- Rate limit each sender to 15 SMS/minute
  - Necessary to limit spam for the 15-30 mins required for new spam content to be identified
  -
- Content filters block known spam text
  - Spam text identified by 7726 reports, heuristics and human analysts

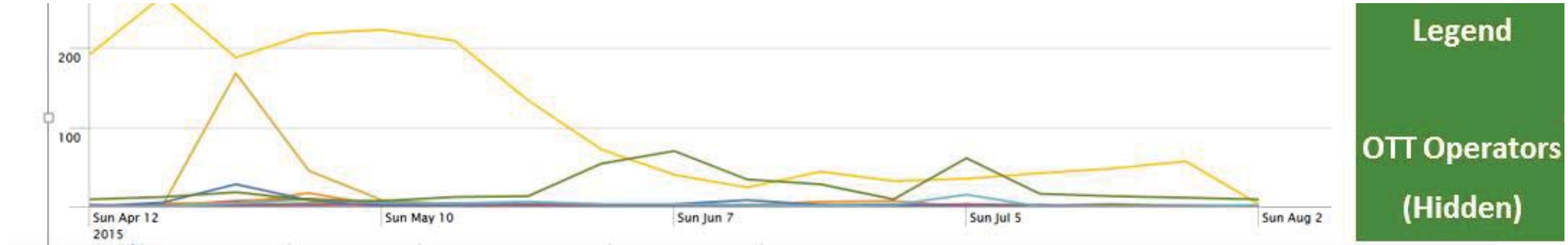


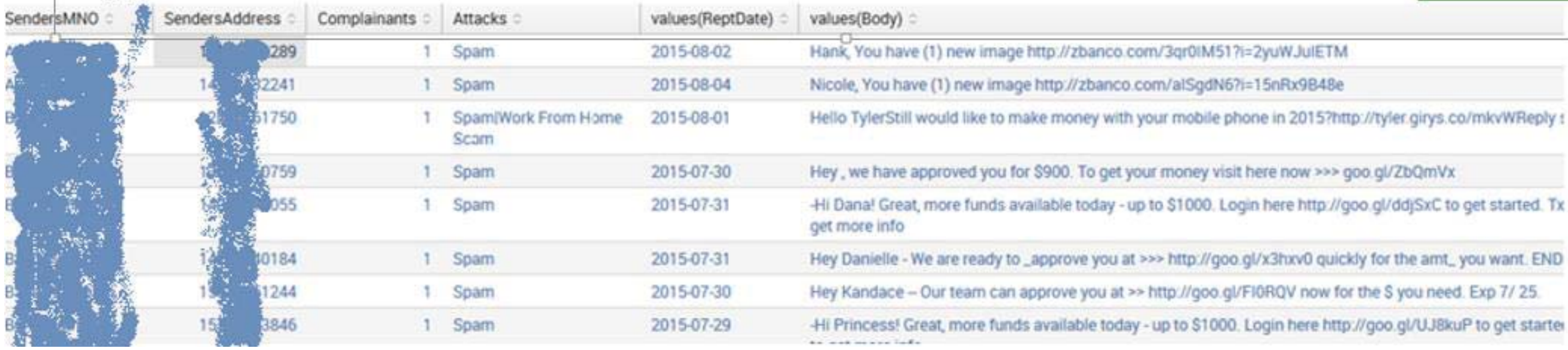



Layered Defense Architecture
Message Flow
Reputation filters (Blacklist)
Volumetric filters (15 msg/min/TN)
Content filters

Q3 2015 OTT Update

- OTT "Snowshoe" methods becoming more extreme
  - 1,500 numbers sending for a single spam campaign
  - Each sends low volumes (1-3 msg/day)
- OTT complaint volume is down
  - Chiefly due to very aggressive AT&T blocking (over 1400 numbers in a day)
  - Spammiest OTT service providers still not using spam filters





SendersMNO	SendersAddress	Complainants	Attacks	values(ReptDate)	values(Body)
[redacted]	[redacted]289	1	Spam	2015-08-02	Hank, You have (1) new image http://zbanco.com/3qr0IM51?i=2yuWJulETM
[redacted]	[redacted]2241	1	Spam	2015-08-04	Nicole, You have (1) new image http://zbanco.com/alSgdN6?i=15nRx9B48e
[redacted]	[redacted]51750	1	Spam|Work From Home Scam	2015-08-01	Hello TylerStill would like to make money with your mobile phone in 2015?http://tyler.girys.co/mkvWReply s
[redacted]	[redacted]0759	1	Spam	2015-07-30	Hey , we have approved you for $900. To get your money visit here now >>> goo.gl/ZbQmVx
[redacted]	[redacted]055	1	Spam	2015-07-31	-Hi Dana! Great, more funds available today - up to $1000. Login here http://goo.gl/ddjSxC to get started. Tx get more info
[redacted]	[redacted]0184	1	Spam	2015-07-31	Hey Danielle - We are ready to _approve you at >>> http://goo.gl/x3hxv0 quickly for the amt_ you want. END
[redacted]	[redacted]1244	1	Spam	2015-07-30	Hey Kandace – Our team can approve you at >> http://goo.gl/FI0RQV now for the $ you need. Exp 7/ 25.
[redacted]	[redacted]3846	1	Spam	2015-07-29	-Hi Princess! Great, more funds available today - up to $1000. Login here http://goo.gl/UJ8kuP to get starte

Originating Service Provider Role

- Spam is best controlled at the source
  - Most attacks originate from ‘suspicious’ and/or related accounts
  - Account information such as login IP address, credit card and date of creation is available only to the originating service provider
  - Spam is less dispersed, more easily identified at the source

- Industry ‘best practices’ document tells service providers how to control their spam emissions

M3AAWG Mobile Messaging Best Practices for Service Providers

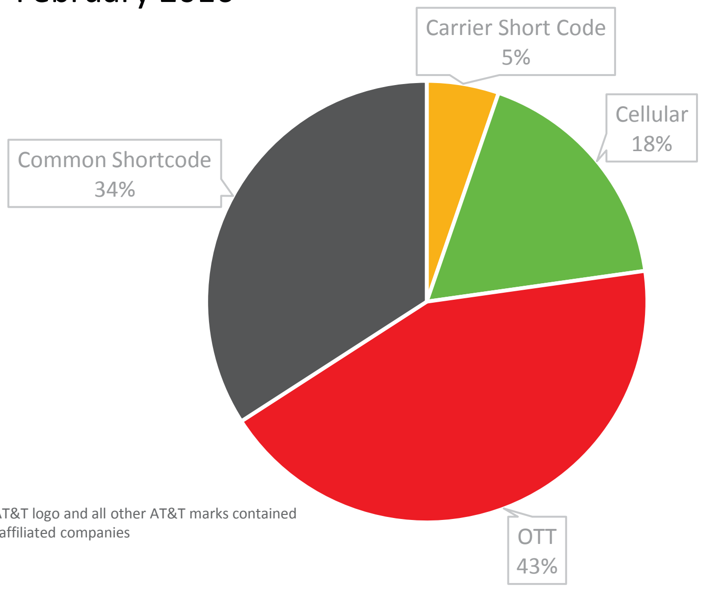
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

- Not all service providers are containing their spam emissions

Over-The-Top (OTT) Spam Status

- **Spammers have returned, using OTT service providers offering Internet APIs**
  - **Internet anonymity (little or no vetting)**
  - **Low costs**
- **Typical spam rates are disproportionate:**
  - **OTT: 2-30%**
  - **Wireless: < 0.1%**
- **Some OTT service providers have stellar records**
- **Some do not**
- **Most short code spam comes from 'shared' short codes where the vetted owner chooses to allow unvetted or poorly vetted parties to send**

Spam Complaints by Source
February 2016



Spam Blocking Statistics

- **AT&T Daily Mobile Terminated (MT) messages: ~750,000,000**
- **AT&T Daily blocked MT messages: 760,000 (~ 0.1%)**
  - 400,000 are OTT
  - 360,000 are Wireless
- **Typical OTT:**
  - 5,200,000 MT msg/day
  - 117,000 MT msg/day blocked (2 ¼ %)
    - 101,000 due to spam text content
    - 16,000 due to exceeding 15 msg/min message rates
- **Typical Wireless:**
  - 159,000,000 MT msg/day
  - 42,000 MT msg/day blocked (0.02%)
    - 41,000 MT msg/day blocked for exceeding rate limits
    - 500 msg/day blocked for spam content

AT&T, June 2012

Spam Filter Operational Incidents

- **Feb 2016 “False Positive” blocking incident: operational error**
  - AT&T spam vendor mistakenly classified several legitimate domains/URLs as spam
  - Messages mistakenly blocked
  - High-volume A2P senders of mistakenly-blocked phone numbers blacklisted
  - Initial blacklist reversal effort incomplete missed some phone numbers
  - AT&T became aware, and promptly requested and escalated requests to unblock

How to Send A2P Messages Reliably

A Story of Openness vs Security Trade-offs

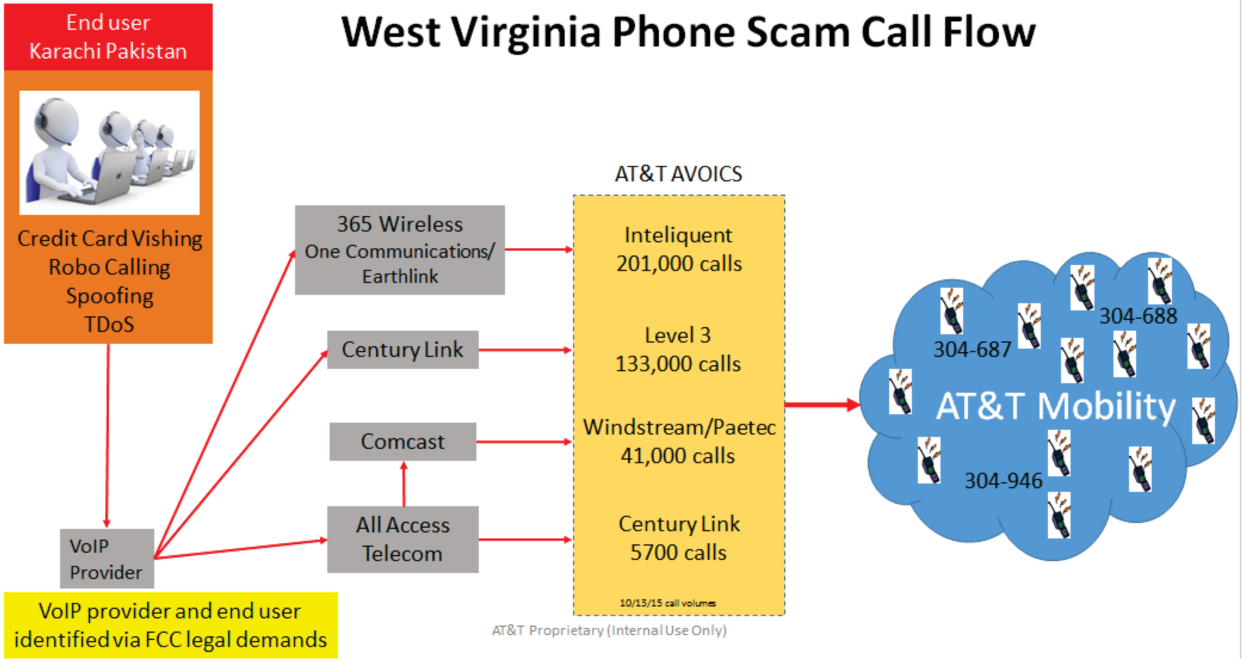
- **Agreements/guidelines**
  - CTIA guidelines: long codes for P2P, short codes for A2P
  - Industry Best Practices for Text Messaging Service Providers (M3AAWG)
- **Existing ecosystem**
  - Long-code ecosystem built for P2P messaging
    - Open access, low cost
    - Spam mitigation requires rate limiting (e.g., 15 msg/min)
  - Short codes for A2P
    - Strict vetting, higher costs, start-up delays
    - High sending rates
- **Industry is working on a new long code A2P framework (CTIA)**
  - Authorized long codes must be identified to permit high rates
    - (requires new infrastructure)
  - Message class(es) and vetting rules must be defined

Spam Blocking Without Regulation

- **Goal: Maximum openness**
- **Email – a functional ecosystem**
  - All (or nearly all) operators filter inbound and outbound messages
    - Often without explicit consent typically with limited user control
  - Advertisers hire specialist companies ("senders") to properly send
  - Sender reputation tracked
  - Harsher policies applied to irreputable senders
  - Bad senders are blocked
- **SMS**
  - Long code (available anonymously) messages are filtered, 15 msg/min maximum per line
    - Filtered without explicit consent or control
    - Reputation is tracked
    - Harsher spam policies are applied to irreputable service providers
    - Bad telephone numbers are blocked
    - In extreme circumstances bad service providers are blocked
  - Short code (vetted), A2P with high rates permitted
    - Extensive vetting of applicants (e.g., statement of authorized use, credit history, ID)
    - Monitored and shut down if abused
    - Shared short codes where owners' customers are not vetted have spam problems

2015: DoS Attack Wiped Out Whole Town's AT&T Voice Service

Regulation Without Spam Blocking



West Virginia Phone Scam Call Flow

End user
Karachi Pakistan

Credit Card Vishing
Robo Calling
Spoofing
TDoS

VoIP Provider

VoIP provider and end user identified via FCC legal demands

365 Wireless
One Communications/
Earthlink

Century Link

Comcast

All Access Telecom

AT&T AVOICS

Inteliquent
201,000 calls

Level 3
133,000 calls

Windstream/Paetec
41,000 calls

Century Link
5700 calls

10/13/15 call volumes

AT&T Mobility

304-687

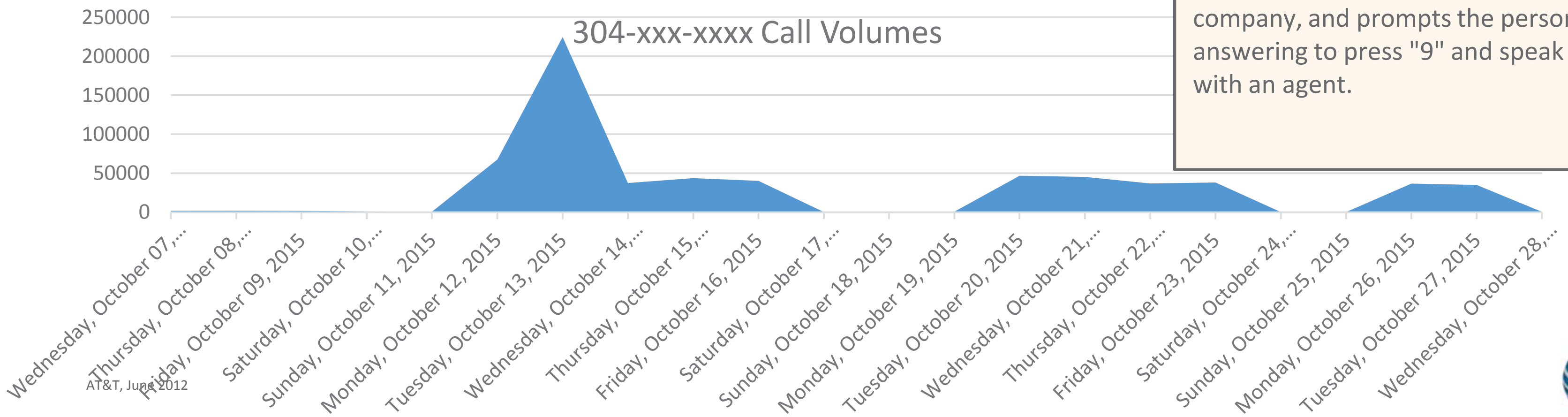
304-688

304-946

AT&T Proprietary (Internal Use Only)

13 WOWKTV.COM
13 NEWS I WORKING FOR YOU

CHARLESTON, WV - CHARLESTON- This isn't just your average phone scam. Hundreds in West Virginia subjected to 100, even 200 phone calls in a single day from a group claiming to be a credit card company. **Customers are getting calls every two or three minutes – all day long.** The organization claims to be "Leslie" or "Lisa's" credit company, and prompts the person answering to press "9" and speak with an agent.



304-xxx-xxxx Call Volumes

AT&T, June 2012